PROCEDURE 1350.90

Issued Date: April 30,2006
Effective Date: May 31, 2006

SUBJECT: **Secure Disposal of Installed and Removable Digital Media**

APPLICATION: This procedure applies to all Executive Branch Departments, Agencies, Boards or Commissions that use digital media of any kind to store information, including all equipment owned or leased by the agency that has memory such as personal computers, Personal Digital Assistants (PDAs), routers, firewalls and switches and other media, such as, tapes, diskettes, CDs, DVDs, worm devices, and Universal Serial Bus (USB) data storage devices.

PURPOSE: The purpose of this procedure is to prevent the unintentional and unauthorized use or misuse of state information and promote the privacy and security of sensitive and/or confidential information resources within the State by defining the minimum requirements for the removal of data from an agency's computer hard drives and electronic media resources prior to their being surplused, transferred, traded-in, disposed of, or the hard drive is replaced. The procedure will also foster state agency compliance with federal regulations dealing with the confidentiality of personally identifiable information; such as the Health Insurance Portability and Accountability Act, the Gramm-Leach-Bliley Act (also known as, Financial Services Modernization Act), and the Family Educational Rights and Privacy Act.

CONTACT AGENCY: Department of Information Technology (DIT)
Office of Enterprise Security

TELEPHONE: 517/241-4090

FAX: 517/241-2013

SUMMARY: This procedure requires proper disposal, transfer, or destruction of State information contained in removable, portable, or installed media containing protected data by defining minimum requirements for the removal of data from an agency's computer hard drives and electronic media resources prior to their being surplused, transferred, traded-in, disposed of, or the hard drive is replaced.

APPLICABLE FORMS: None [unless a defined tag to mark cleansed equipment would help]

PROCEDURE:

A. Information security risks can be created by reassigning, surplusing, transfer, trade-in, disposal of computers, or replacement of electronic storage media, and computer software without ensuring the proper disposal of installed and removable digital storage. These risks may include:

1. Violation of software license agreements,
2. Unauthorized release of sensitive and/or confidential information,
3. Violation of federal laws including but not limited to the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act of 1996 (HIPAA), The Family Educational Rights and Privacy Act (FERPA), etc., and
4. Unauthorized disclosure of trade secrets, copyrights, and other intellectual property that might be stored on the hard disks and other storage media.

B. Agency responsibilities:

1. Ensure compliance with the Record Retention and Disposal Schedule before following this procedure.
2. Whenever licensed software on any computer media being surplused, transferred, traded-in, disposed of, or the hard drive is replaced, the terms of the license agreement shall be followed.
3. All hard drives (this includes instances where equipment has multiple hard drives) and electronic storage media shall have all state data properly removed prior to disposal or release.
    a. This does not apply where the equipment is being transferred or re-assigned within the same agency with a specific intent to also transfer the software and data.
4. Data removal procedures shall be properly documented in accordance with this procedure and in accordance with any software manufacturers' guidelines to prevent unauthorized release of sensitive and/or confidential information that may be stored on that equipment and other electronic media.
5. Agencies may comply with this procedure by:
    a. Disposing of the data themselves,
    b. Using a media disposal contractor certified to ensure adequate security controls and destruction of data, or
    c. Seeking the technical assistance of DIT to do the cleansing.
6. Maintain a record of compliance with this procedure, and tag equipment as having had the data removed. The record shall include the following information:
    a. The method(s) used to expunge the data from the storage media.

b. The type of equipment/media from which data was removed.
c. The name of the person responsible for the removal of the data.
d. The name and signature of their supervisor.

7. Make Contractors and third party providers of data operations and services to the State of Michigan aware of the requirements of this procedure and require their compliance by contract language and oversight.
    a. Ensure proper disposal of digital information contained on the media installed on equipment operated by contractors is accomplished.
        i. Agencies may meet this requirement by mandating the return of the storage media. Use of registered mail or process to establish chain of custody is required to ensure adequate accountability during transit.

C. DIT responsibilities:

1. Define acceptable methods to remove and cleanse digital media of data in a manner that gives assurance that the information cannot be recovered.
    a. Agencies may use the following methods to completely erase or make data unreadable:
        i. Three passes with a disk wiping utility or DOD Level 2 compliant equal.
        ii. When magnetic tape or optical media is to be reused, it should be completely emptied of data and prepared by software tools designed to securely erase and/or completely reformat the media,
        iii. Physical destruction
            a. Incineration,
            b. Shredding,
            c. Cutting, drilling, or grinding,

        By such other method recommended by the manufacturer for devices such as personal computers, PDAs, routers, firewalls and switches where DIT is satisfied the method will cleanse all state protected data.
    b. Before the removal process begins, the computer shall be disconnected from any network to prevent accidental damage to the network operating system or other files on the network.
    c. An "erase" feature (e.g., putting a document in a trash can icon) or deleting a file is not sufficient for sensitive

information because the information may still be recoverable.

d. Disposal of digital media shall be done in accordance with all applicable State or Federal surplus property and environmental disposal laws, regulations or policies.
e. When external entities or contractors are used to accomplish disposal, a log shall be maintained for audit containing, at a minimum:
    i. The serial number(s) and asset tag number of the equipment
    ii. Tag numbers of all media delivered
    iii. The name of the person receiving the state assets for disposal
    iv. A signed receipt.

2. Certify fully functioning implementation of access as authorized.
3. Certify compliance with established IT security policies, standards and procedures.
4. Through DIT Office of Enterprise Security, review and monitor procedure to ensure appropriate authorization methods are implemented and take actions necessary to ensure compliance with State of Michigan IT security policies, standards, and procedures.
5. Through Internal Auditor, conduct periodic audits of IT resources for appropriate controls to maintain compliance with policy and standards.

D. Unique digital data storage situations not obviously covered by this procedure should be coordinated with DIT, Office of Enterprise Security, Risk Management Division.

E. The policy described in this section sets a minimum level of conformance that will be implemented across the Enterprise. State Departments desiring to implement more stringent practices and procedures for their information technology environments may do so with the approval of the Office of Enterprise Security.

Authority is The Management and Budget Act, Public Act 431 of 1984, as amended, § 203.

* * *